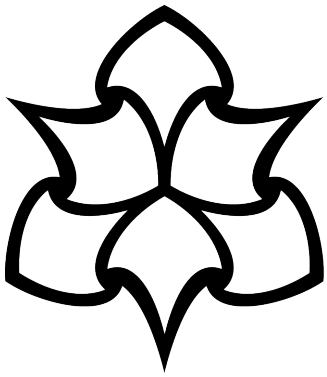

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 30, 2021, accepted February 13, 2021, date of publication February 23, 2021, date of current version March 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3061411

On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities

GEETANJALI RATHEE[1], RAZI IQBAL[2], (Senior Member, IEEE), OMER WAQAR[3], (Member, IEEE), AND ALI KASHIF BASHIR[4], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat 173234, India
[2]Department of Computer Information Systems, University of the Fraser Valley, Abbotsford, BC V2S 7M8, Canada
[3]Department of Engineering, Thompson Rivers University, Kamloops, BC V2C 0C8, Canada
[4]Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, U.K.

Corresponding author: Razi Iqbal (razi.iqbal@ieee.org)

This work was supported in part by the Tomsk Polytechnic University, Russia, through the Competitive Enhancement Program, under Grant VIU-ISHITR-180/2020, in part by the Sri Lanka Technological Campus, Sri Lanka, Seed under Grant RRSG/20/A7, and in part by the Research Fund, Thompson Rivers University, BC, Canada.

ABSTRACT A smart city refers to an intelligent environment obtained by deploying all available resources and recent technologies in a coordinated and smart manner. Intelligent sensors (Internet of Things (IoT) devices) along with 5G technology working mutually are steadily becoming more pervasive and accomplish users' desires more effectively. Among a variety of IoT use cases, e-voting is a considerable application of IoT that relegates it to the next phase in the growth of technologies related to smart cities. In conventional applications, all the devices are often assumed to be cooperative and trusted. However, in practice, devices may be disrupted by the intruders to behave maliciously with the aim of degradation of the network services. Therefore, the privacy and security flaws in the e-voting systems in particular lead to a huge problem where intruders may perform a number of frauds for rigging the polls. Thus, the potential challenge is to distinguish the legitimate IoT devices from the malicious ones by computing their trust values through social optimizer in order to establish a legitimate communication environment. Further, in order to prevent from future modifications of data captured by smart devices, a Blockchain is maintained where blocks of all legitimate IoT devices are recorded. This article has introduced a secure and transparent e-voting mechanism through IoT devices using Blockchain technology with the aim of detecting and resolving the various threats caused by an intruder at various levels. Further, in order to validate the proposed mechanism, it is analyzed against various security parameters such as message alteration, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack and authentication delay.

INDEX TERMS Blockchain, trust-based e-voting, blockchain e-voting, smart cities.

I. INTRODUCTION

The accelerated pace of urbanization in the recent decades has endangered the environment and economic sustainability by raising several social, technical and economic concerns. Therefore, for exploiting and optimizing the tangible and intangible assets, governments across the world have been taking an interest in adopting the concept of smart cities and its related infrastructure [1]. A smart city refers to an intelligent environment obtained by deploying all available resources and technologies in a coordinated and smart manner with the means of developing urban centers [2], [3]. Further, for advancing the well being of individuals (such as public, government and other stakeholders), better utilization of resources and enhanced performance of city operations, a smart city uses data and recent techniques to align institutional, physical, technical and social elements of the city. Traffic management, smart industry, smart grid, smart healthcare, public safety, secure e-voting and water management are the various developments related to smart cities that are being retro fired with IoT and smart sensors.

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wu.

Further, intelligent sensors and recent technologies working mutually are steadily becoming more pervasive and accomplish users' desires more effectively and efficiently. Objects with internet protocol (IP) connectivity are correlated to the internet to offer better usability in day-to-day actions. Further, this interconnection amid devices creates a lot of data such as device status, energy usage and environmental behavior that can be aggregated, composed and then disseminated in an adopted, confined and secure manner. Moreover, as these devices are associated to the internet, they can be controlled at anytime and from everywhere. Therefore, the goal of smart cities is to make best public resource usage with improved services and quality of life by using advanced communication and information technology. Further, in order to ensure a reliable data exchange among devices, there is a need to use massive communication capabilities such as 5G, *and* 6*G* technologies [4], [5].

A. RESEARCH SIGNIFICANCE

According to 5G technology provides an efficient transmission and collaboration of data as it includes super IoT, mobile ultra broadband and artificial intelligence, providing enhanced connection capability and terabits transmission in seconds by optimizing the network smartly [6]. However, with the usage of 5G technology, the huge volume of data generation, processing, sharing, analyzing and storing leads to a number of privacy and security concerns such as identify theft and/or Denial of Service (DoS), man-in-middle attack etc. Future research in this technology is crucial for the advancement of IoT technology in general and smart cities in particular. Recently, of the various smart city applications, e-voting has pioneered to aid intelligent decision making for a range of physical objects vital to the experimental growth in an efficient and effective manner [7]. Among a variety of IoT use cases, e-voting is a considerable application of IoT that relegates it to the next phase in the growth of technologies related to smart cities and provides intrusion-free democratic procedures for the citizens of these cities [8], [9]. The principle of e-voting is to cast or count the votes using some electronic means and connect the various participating entities via a secure mechanism so that any alteration with data or votes at any level is easily detected [10], [11]. Another motive of smart e-voting technique is to provide a transparent and meddling-free election process to the voters who are notified at each step as their votes are processed. The inconsistencies and redundancies in the voting process are successfully identified by replacing article based mechanism with advanced IoT devices that are interconnected. The smart e-voting mechanism in addition to being secure and reliable also provides effective use of resources and means as depicted in Figure 1. The present Figure 1 determines the benefits of using blockchain based vote casting system by providing the transparency at each level of e-voting.

While discussing these applications we need to focus on the issues and threats related to IoT devices that need to be tackled for better adoption and incorporation of these

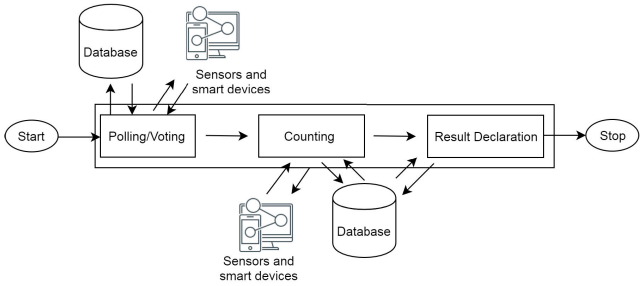

FIGURE 1. E-Voting architecture.

intelligent objects in smart city environments [12], [13]. The existing IoT devices responsible to gather information from diverse resources extend the attack surface by creating an initial entry point for malevolent attackers to intrude in the system [14]–[16].

B. BLOCKCHAIN IN E-VOTING

According to the latest studies, IoT devices are increasing at such an exponential rate that in future they may be seen exactly situated at the heart of the smart city solutions. Therefore, it is much needed to solve the security requirements and service quality of various IoT applications. While IoT devices have several benefits to society, many organizations and businesses are still cautions to use them. Lately, majority of the IoT devices are being used as messaging applications with its easy features and centralized communication structure. Numerous IoT elucidations are rather costly due to expenses associated with centralized clouds, when such a frame is not created by the traders, the cost emits from intermediates. In conventional applications, all the smart devices are often assumed to be cooperative and trusted. However, in practice, IoT devices may behave as malicious devices (MD) with the aim of disrupting the network services. The privacy and security flaws in the e-voting systems in particular lead to a huge problem where intruders may perform a number of frauds for rigging the polls [17]–[19]. Thus, the potential challenge is to distinguish the ideal IoT devices from the malicious ones in order to establish a legitimate communication environment. Further, in order to prevent from future modifications of data captured by smart devices, a Blockchain is maintained where blocks of all legitimate IoT devices are recorded [20], [21]. Blockchain technology can meet the demand for transparency, request for which is increasing at an astounding pace. In addition, it can ensure security and transparency among the devices even though IoT objects may be hacked by intruders as any alteration with the data can be easily detected. Further, Blockchain technology can be used to track, organize and support communications by storing the data from many devices and facilitating the formation of parties without any centralized cloud.

C. CONTRIBUTION AND MOTIVATION

This article has introduced a secure and transparent e-voting mechanism through trusted IoT devices using Blockchain

technology with the aim of detecting and resolving the various threats caused by an intruder at various levels. The trust of IoT devices are computed through a social optimizer that identifies their trust values by analyzing their communication behaviours. Further, Blockchain technology plays a crucial role in coordinating the activities of legitimate IoT devices in the proposed solution. In order to prevent a prospective change of stored record of votes in databases, Blockchain is maintained at various levels that keeps track of all the recorded information handled by the election conducting bodies. Therefore, the potential contribution of the proposed framework is detailed as follows:

1) The security of IoT devices is ensured by analysing their communication behaviours through social optimizer by ensuring their trust values.
2) The proposed mechanism is a two end system, i.e., both the National election bodies and every entity may ensures the security upon compromise of IoT devices through blockchain mechanism.
3) The proposed mechanism of voting using Blockchain not only serves the election conducting bodies but also the voters who get notified in case of any meddling with their votes before the scheduled counting day.

The rest of the article is organized as follows. The related work of secure e-voting with and without Blockchain mechanism is detailed in section two. A secure smart e-voting mechanism using Blockchain technology is discussed in section 3. Further, section 4 and 5 detail the performance analysis and experimental results against various metrics. Finally, section 6 concludes the article with future directions.

II. RELATED WORK

The traditional article based voting systems or mechanism may leads to climate deterioration and forest destruction. Therefore, in order to resolve this issue, the article based systems are replaced with smart e-voting processes. Hence, to ensure a secure voting mechanism, [22] have proposed a rank choice e-voting mechanism by eliminating hardwired restrictions. For ensuring the vote's confidentiality, every vote is encrypted through ELGamal process. Further, the proofs are generation upon storage of each vote that further verifies the counting process without decrypting the content. The proposed mechanism is validated by showing the experimental results in comparison of existing mechanisms. The encryption and decryption of content at each node may lead to increase the computational and communicational overhead in the network. Further, in e-voting system, it is necessary to ensure the security of candidates who cast their votes and transmits information. [23] have proposed a crpto-biometric approach for online voting mechanisms. The palm vein and palmprint are the two major crypto-biometric methods of proposed mechanism where the authors have used gabor filter with a threshold measure. In addition, the transmitted information is being encrypted through a random key after embedding in biometric vector through a fuzzy commitment method. The decryption process is done by extracting the encrypted key using new retrieval method. The results validates the crypto biometric system in terms of key retrieval and accuracy. Furthermore, [24] have illustrated the transparency and organizations mechanism of nationwide e-voting in the context of security concerns and requirements. The authors have discussed a case of brazil pioneering the nationwide adoption of voting over 20 years ago. Though the article less conduction of voting enhances the convenience and accessibility to the users located in far away countries. However, the article less e-voting systems leads to severe security risks such as verifiability, integrity, voter's unlink ability. Further, authenticity and votes manipulation are the two major security concerns in e-voting applications in order to validate the legitimate voter during election process. Several researchers have proposed secure e-voting systems, however, none of the methods are practically implemented due to light weight computing machines. The [25] have proposed a verified and secured polling mechanism using cryptographic approach to ensure vote's integrity and voter's identity. The multifactor authentication mechanism prevents double voting uncoercibility and verifiability of the untrusted individuals. The proposed mechanism is validated by showing a practical and verifiable pooling mechanism. However, double verification process with key management and storage overhead further leads to complex computational. [26] have proposed a secure e-voting mechanism integrated in a single framework by addressing materialization, receipts, uniqueness, voter's anonymity and privacy. The proposed approach viability is presented through a election markup language and web service. However, a complete transparency is not provided by the system to the voters.

In order to ensure transparency and privacy of the individuals, E-voting system must be completely reliable and secure. [27] have implemented an e-voting application using solidity and Ethereum language where the task of Ethereum Blockchain is to keep the individual's ballots and vote's record. Further, the users are permitted to cast their votes through wallet android application using consensus. In addition, the efficiency and reliability of Blockchain enabled e-voting is presented through various simulation results. In order to increase the voting percentage and reduce various frauds during polling and voting systems can be easily handled through Blockchain mechanism. However, they have not discussed the security threats that can be encountered by the intruders through IoT objects. [8] have proposed a smart e-voting system where individuals may cast their votes through Smartphone or laptops. The e-voting mechanism using Blockchain technology have used tamper proof secret identities and encrypted key processes for ensuring the transparency and security in the system. The article has pointed out certain implementations, challenges and potential benefits of using Blockchain enabled e-voting mechanism. To solve the risks related to voting fairness where individuals may cast their single vote twice, voting of non-candidates, tampered data and excessive authorities, it is necessary to further look over the security concerns of voting systems. The integration

of Blockchain mechanism and voting system may reduces the mentioned risks with transparent and decentralized feature of Blockchain technology. [28] have proposed e-voting Blockchain system to maintain the transparency, limit the voting threats and audit the incorrect voter's operations using hash-based and certificates cryptographic mechanism. However, the proposed mechanism of the authors is suitable in the case where number of voters are less and voting is done at small scale. The security of information is suggested by [29] through a hash based technique by introducing the concept of block creation and sealing. The consortium Blockchain ensures the owner of governing bodies where no one is allowed to access or change any data from the outside. The adjustable Blockchain mechanism illustrates the hash algorithms, information accumulation, block creation and sealing, polling process and result declaration. The author's in this article claimed the detain of data management and security issues by providing an enhanced manifesto of e-voting process using Blockchain technology. However, they have not discussed about the security issues of IoT devices through which polling mechanism can be disrupted by intruders. [30] have surveyed the use of Blockchain application in various fields. The authors have reviewed how Blockchain mechanism can be applied in smart cities from perspectives of smart transportation, smart citizen, smart healthcare, smart e-voting etc. Further, the authors have illustrated a Blockchain based e-voting mechanism consisting of five different steps such as election creation, registration, transaction, tallying and verification. Further, the authors have pointed the challenges and future perspectives in Blockchain mechanism. Though number of authors have proposed various security and blockchain based mechanism in various applications. However, the blockchain based e-voting system is still at its early stages. The goal of this article have proposed a transparent mechanism in order to overcome the existing issues such as cost, time, delay, computational storage, key management overhead etc.

III. PROPOSED TRUST COMPUTATION MECHANISM

Further, in order to identify the legitimacy of IoT devices, the proposed mechanism isolates the malicious devices by eliminating the threats encountered during communication and path formation process by computing the weighted trust of each device. Moreover, to ensure transparency in the polling mechanism, a blockchain is maintained that includes secured IoT devices to further formulate a secure polling process. This article illustrates a secure e-voting use case for smart cities via the use of IoT devices by computing 1) the trust of each IoT device that provides legitimate communication among entities and 2) blockchain mechanism which further maintains and ensures the transparency of IoT devices during polling process as depicted in Figure 2.

A. TRUSTWORTHINESS OF IoT DEVICES

For ensuring a secure communication transmission, a trustworthy approach is needed that can compute the trust of each IoT device by identifying its communication behaviour. Further, the trustworthiness or trust value of each IoT device is determined that generates a secure path through social optimizer by analyzing its communication behaviour. The proposed trusted approach enhances the metrics by reducing cryptographic key management and storage overhead needed during communication process. Further, a dijkstra's shortest path algorithm along with trusted nodes is used to route the packets and ensure the security to each IoT device. The reason for choosing dijkstra's algorithm is easy implementation for path formation and generation process by considering their positive weights. In addition, the trust of each IoT device is computed using various networking parameters where IoT device trust is finalized through social rank mechanism. For using the dijkstra's mechanism, the weights are associated to each device for path computation among entities that are evaluated through several parameters such as packet loss, remaining energy, device trust and device distance as discussed below:

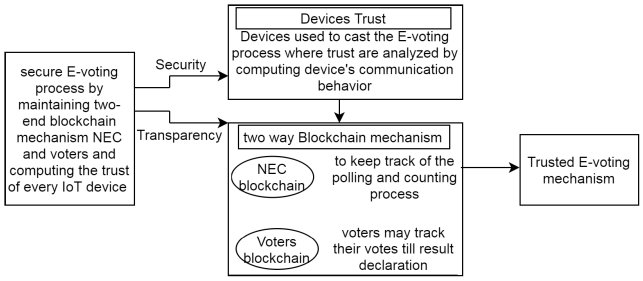

FIGURE 2. Holistic flow of proposed phenomenon.

1) *Packet Loss (PL)*: it can be occurred due to internal threats either intensive or genuine. During the traffic congestion and network delay, the packet loss can occur that are considered genuine while intensive packet loss encountered by the intruders who intensively wants to drop the packets as defined in equation 1:

$$PL = \sum_{i=1}^{N} (PKT_{received} - PKT_{transmitted}) \quad (1)$$

2) *Remaining Energy (RE)*: it is computed as the amount of energy remains by every IoT device after forwarding or broadcasting the data packets. Node's energy is considered as a very important parameter of node's trust as malicious devices consumes and presents huge amount of energy to attract the genuine nodes in the network. The RE is computed as equation 2.

$$RE = TotalEnergy - (E_r - E_t) \quad (2)$$

3) *Device distance*: it computes the distance among two nodes to analyze the energy transmission and packet delivery through Euclidean distance formula as equation 3:

$$DD_{(i,j)} = \sqrt{((x_i - x_j)^2) + ((y_i - y_j)^2)} \quad (3)$$

4) *Device Trust (DT)*: The trustworthiness of each IoT device is computed through SITO that depends upon previous communication and transmission interaction. For trust computation, each device rank is calculated through RE and PL as equation 4:

$$DT = \sum_{i=1}^{N} (Previous\ node\ interaction) \tag{4}$$

Initially, a random trust value is assigned that increases or decreases depending upon the social rank. However, in order to compute the trustworthiness of each IoT device during communication or transmission process, the weight of each node is summation of different parameters as defined in equation 5: The below equation 5 illustrates the updating of node's weight depending upon their communication behaviour. The node's having higher weight leads to highly trusted node and take part in further communication process in the network.

$$W_d = \sum_{i=1}^{N} (RE + PL + d_{x,y}) + TV) \tag{5}$$

A social rank optimizer is used to compute the legitimacy or malicious behaviour of each node by analyzing its trust value. The device whose trust value is above a threshold parameter may further involve in communication process of e-voting mechanism. Further, the proposed mechanism ensures a transparency to election process and voters by tracing each and every activity of the polling process.

B. BLOCKCHAIN E-VOTING USING TRUSTED IoT DEVICES

In smart e-voting systems, transparency of votes, election management, voter registration and voter verification are managed independently in a decentralized environment via a Blockchain mechanism. In traditional systems, any illegal activity (or rigging) at one location is completely out of knowledge of the managing authorities i.e. National and State-level Election bodies which poses a serious threat to an efficient democratic voting. Transparency is the most important factor to determine a free and fair election and ensure that people's choice has been exercised. Using a Blockchain mechanism all the transactions are clearly visible to the election bodies at every level. Also, the voters are notified regarding the status of their votes which boosts people's faith, further strengthening democratic institutions. Although several approaches have been proposed to ensure transparent and secure e-voting, however, there are several issues that still exist at various levels such as multiple fake registrations of a voter at more than one place and infringement with votes before the day of counting that need to be tackled. Usually, the Election conducting body at the national level overlooks the entire polling process subordinated by state level bodies using a systematized mechanism. Though the entire election process is handled via IoT devices, However, these systems can be easily compromised and distorted by doing some malevolent activity at a particular level. Even though, the activities may be captured through smart devices, still it is very critical to trace each and every activity at all the levels. In the proposed solution, all the activities are managed using a Blockchain based mechanism. We have proposed a two end mechanism in which all the activities are coordinated by the national and state bodies at various levels and voters play an equal part in it. The scope of this article is to provide a secure hybrid voting architectural framework using Blockchain technology.

C. SYSTEM MODEL

This section describes the system model of the proposed framework. The hypothetical situation as depicted in Figure 3 consists of a national election body called as National Election Commission (NEC) which initiates the election process. It directs and coordinates the working of several State Election commissions (SEC) in a centralized manner. These SECs overlook the election process in the various districts within their boundaries. The districts within a state have various subsidiary district level election bodies which overlook the smooth functioning of an election in their respective districts. A district further consists of several polling booths where voters cast their votes. The Voters make up the final level of the hierarchy of the architecture. When an election is underway, the NEC has all the rights to over look each and every activity and data not only at the state level but also at the level of polling booths via the Blockchain thus removing the possibility of rigging at the SECs. The decentralized architecture of the mechanism paves way for each entity to look in every other entity's database further boosting lucidity. A key feature of the system model is that a secret key is issued to each voter using which he/she can ensure that the vote has not been meddled with.

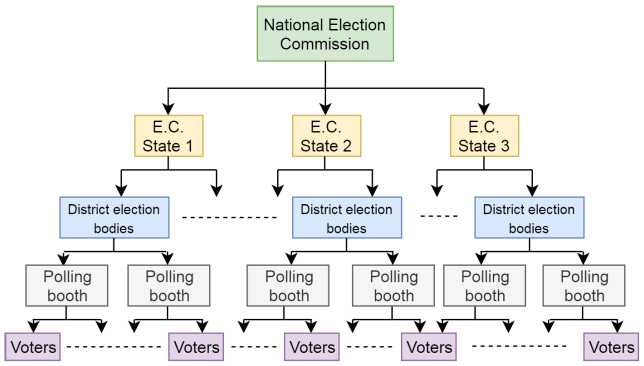

FIGURE 3. Level-wise E-voting mechanism.

D. WORKING OF PROPOSED SOLUTION

While working with smart systems particularly in healthcare and industries usually a permission blockchain is implemented to protect the privacy of the data at various levels. However in e-voting systems a permission free blockchain is very important in order to avoid meddling and rigging and maintain a free and fair election for modern democratic systems. In the proposed system model, a hierarchical

architecture as depicted in Figure 3 has been implemented which can be understood at three levels.

Level 1: Initially a Blockchain is setup by the NEC which is the supreme authority for monitoring the elections for the entire country. The NECs direct and coordinate the activities of State level Election Commissions which are responsible for smooth conduct of elections within their boundaries.

Level 2: Next, the several district levels subsidiary election bodies of various states are added to the Blockchain which manage the process of polling in their respective districts and report to the SECs.

Level 3: The final level consists of the various polling booths located in a district where voters cast their votes. When a voter casts a vote, a secret key is generated for each voter on the basis of his/her biometrics and the same is displayed in the database of all the entities.

When a voter 'X' successfully casts the vote, it is reflected in the Blockchain after the verification of his/her biometrics. Since the biometrics of the voter are checked before casting, any person trying to re-cast vote or try to disrupt any IoT device in another district or state is immediately caught as it is already highlighted in the database of all the parties involved at district and state level that the vote for these biometrics has been casted instead of just the allotted polling booth as depicted in Figure 4.

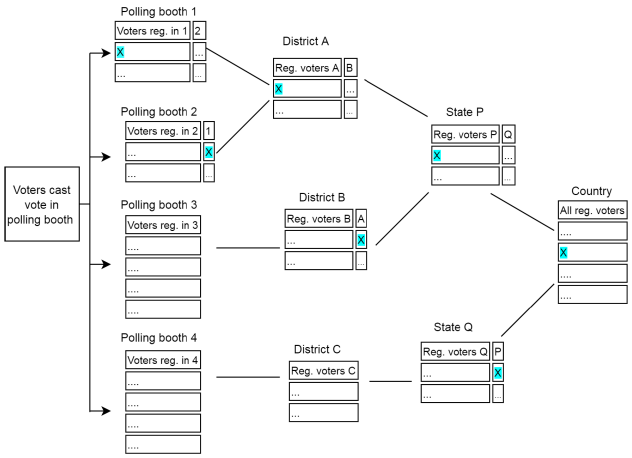

FIGURE 4. Blockchain mechanism in E-voting.

Further, as depicted in Figure 4, the working of the model is as follows, various voters cast their votes at polling booths 1 and 2 located in district A, polling booth 3 located in district B and polling booth 4 located in district C. Let districts A and B are located in State P and district C be located in state Q. All the polling booths of a particular district can view each other's data while all the districts of a state have access to the database of all the other districts of that particular state. The states in turn have access to the information of voters in all the other states while the NEC coordinates the entire process.

Any change or meddling in the election process at any level is clearly visible to all the participants of the blockchain and an infringement of data can be clearly pointed out by

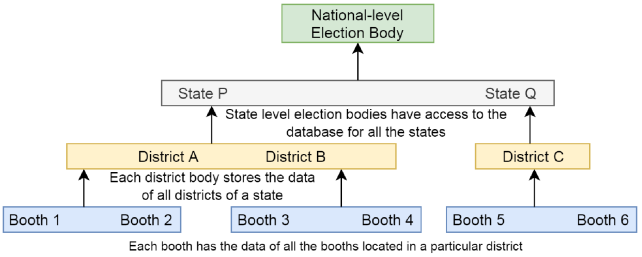

FIGURE 5. E-voting hierarchy.

verifying with the information already registered with the various entities as depicted in Figure 5.

The Blockchain being permission free provides no barrier to the various levels to view each other's data, for e.g. all the SECs have the info of each other's districts and the voters registered in them. It serves dual purpose of providing transparency and avoiding the registration of same voter in more than one state. Now, how the Blockchain handling the various activities through Blockchain is detailed as follows. When a voter casts his/her vote, it gets reflected in the Blockchain to the various polling booths across the district. In order to maintain the principle of secret ballot, the party or person to whom the vote has been cast is not shown at any level. All such votes from various polling booths across various districts are visible not only to their respective state but to all the states that are part of the Blockchain. Any voter found registered in more than one district or state is considered illegitimate and the vote casted stands cancelled. An algorithm of Blockchain E-voting polling system using trusted IoT devices are given as Algorithm 1, Algorithm 2 and Algorithm 3.

E. TRACE ABILITY OF LEGAL ACTIVITIES AT VARIOUS LEVELS

In order to prevent and control illegal activities regarding the polling process by disrupting the IoT devices, Blockchain technology plays a significant role. Even if all processes including vote casting, vote counting and result are recorded, a malicious entity or IoT device may try to steal or alter the stored data. Sometimes in traditional systems these activities may remain unrecognizable. However if mechanism is performed via a Blockchain, entire data is stored in the database of all the entities or IoT devices and an infringement with data may be clearly visible to all, thus bringing down cases of rigging and meddling.

F. WHEN A CITIZEN CASTS A VOTE

Traditionally when a person casts a vote, its processing is kept hidden from all the entities and the counting is done under the supervision of local election authorities. Further, the compiled results are sent up the hierarchy to the district and then the respective SECs which function under a NEC. It involves high risk of interference at every level as each level is independent and though secrecy is maintained, any infringement with the votes may remain hidden from the voters. The cases

Algorithm 1 Algorithm of Secured E-Voting Using Trusted IoT Devices

1: **Input:** A network 'n' consist of 'd' number of IoT devices
2: **Output:** The IoT devices are either legitimate or malicious
3: *Step 1:* Trustworthiness of IoT devices
4: Compute IoT device trust by computing their weights() **if**(*IoTdevice* == *trusted*) **then**
5:
Compute DDR ()
6:
Malicious devices and not be able to add in the blockchain
7:
8: *Step 2:* E-voting process through legitimate IoT nodes (*IoTdevice* == *legitimate*) **then**
9:
Maintain Blockchain 1 () that maintain all the voter's record within state, district and polling booth
10: Maintain Blockchain 2 () with list of persons with casted votes
11:
Not allowed to maintain Blockchain 1 () and Blockchain 2 ()
12:

Algorithm 2 Calculation of IoT trust() Through Social Weighted Rank

1: **Input:** The number of transactions/ communications done by each IoT device is computed as per their social rank depending upon certain parameters:

$$W_d = \sum_{i=1}^{N}(RE + PL + d_{x,y}) + TV) \tag{6}$$

if(*IoTdevicetrustisasperthresholdratio*) **then**
2:
Devices are trustworthy
3:
Devices are malicious
4:

of illegitimate voters which register themselves in several districts and states are very high because the various entities in various districts and states cannot share data in real time and cross check the voter's legitimacy.

In order to tackle these issues a smart voting mechanism has been proposed as depicted in Figure 6 which works in the following steps:

Step 1: Initially when the voter casts a vote he/she is verified using his/her biometrics and is provided with a unique secret key. The voter is highlighted in the database of all the entities that the vote has been casted.

Algorithm 3 Calculation of Blockchain ()

1: **Input:** The number of transactions/communications done by each node is maintained as Blockchain
2: *Step 1:* Blockchain 1()
It maintains a chain of all the records stored by national election commission, polling booths, district and states.
3: *Step 2:* Blockchain 2()
It maintains a chain of all the voter's who casted their votes in order to ensure the transparency among voter's counts.

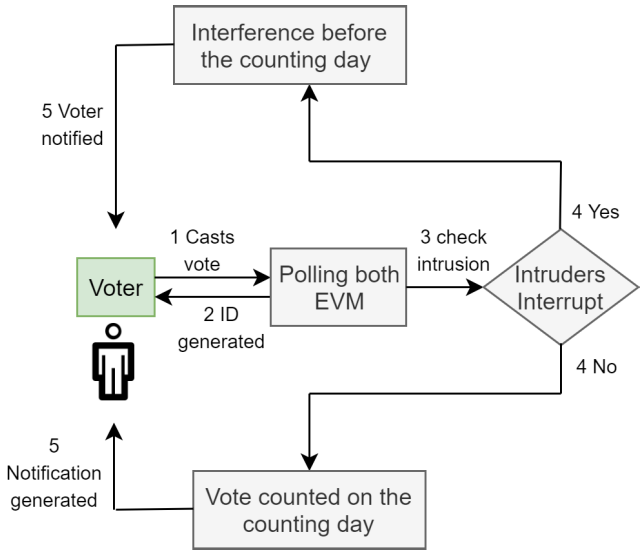

FIGURE 6. Voter casts a vote.

Step 2: If no intrusion or meddling with the vote takes place, the voter is notified on the counting day that the vote has been successfully counted.

Step 3: In case any third party interferes with the vote already cast before the counting day, the voter is immediately notified regarding the same.

As explained in Figure 6, both the process after step 4 will be generated by independent entities for 'n' number of persons'. Therefore, the notification to voters and its generation will be generated at the same step for number of voter's at a single instance of time and the last step can be either notification to voters in case of interference or notification generation in case of vote cast.

G. DOUBLE BENEFITS OF USING BLOCKCHAIN IN E-VOTING

The use of Blockchain in the proposed mechanism is a two end system, i.e. all the entities involved have access to all the data of the Blockchain and the voter can track his/her vote. The Proposed mechanism of voting not only serves the election conducting bodies but also the voters. The major problem faced by election bodies that is being solved is the illegitimate registration of a single voter in more than one state that has

been countered by making the data visible to all the state level and district level bodies via a Blockchain. The benefit provided to the voter is that he/she is ensured that the vote has not been meddled with and has been successfully counted via generation of notifications. The cases of meddling and infringement thus, being reduced enhance transparency in the voting process and establish faith in the democratic institutions crucial for working of modern societies.

IV. PERFORMANCE EVALUATION

This article proposed a secure smart e-voting mechanism using Blockchain which not only ensures a genuine polling system but also builds a trust over election commissions. Initially, a blockchain is created using ethereum platform to validate the proposed phenomenon. Further, to measure the security against malevolent IoT devices where intruders may disrupt certain entities in the network, we have used a MATLAB simulator. The authenticity and security metrics are analyzed upon MATLAB where number of networks are created to identify legitimacy at various levels. Table 1 and Table 2 presents a smart e-voting milieu of 400 m $\times$ 400 m having various number of nodes. Further, the validity of proposed mechanism is proved against considering a malevolent milieu where genuine nodes (such as IoT devices or voters) are compromised by the attackers over MATLAB simulator.

TABLE 1. Simulation Environment of Smart E-Voting

Parameters	Values
Simulation Time	60s
Grid Area	400 $\times$ 400
Number of Nodes	200
Communication Range	120m
Size of Data	IEEE 802.11
MAC	200

TABLE 2. MATLAB Arrangement for Diverse E-Voting Environment

Network	Nodes	Edge Nodes
Network 1	50	10
Network 2	100	15
Network 3	200	20

Furthermore, the MAC is 802.11 with the communication range of 120m of routers. Initially, 50 nodes are formed that operate as IoT devices. Further, a synthesized data creator has been used which creates data using normal delivery of pattern. In addition, the security is measured by embedding malevolent number of nodes through probability distribution during communication mechanism.

Malware, DoS, DDoS and voter authentication are considered as severe routing threats as the former drastically affects the data slumps while later affects the network metrics by consuming the network resources during the communication process. Malware is malicious software which includes spyware, Trojan horse, worms and ransom ware at any point in e-voting path by disrupting to prevent voter's vote from being recorded as intended. DoS threat slow down or interrupt the communication process in the network. It can be used to disrupt vote casting, tallying, auditing phase of e-voting process. Further, the authentication mechanism occurs when system verifies that the communicating entity (voter/person) is the one that it claims to be. The involvement of nodes authentication, malevolent nodes is based upon probability distribution as depicted in Table 3. Initially, 50 nodes are dispensed to each network and after 60s more number of nodes are allotted to verify the structure scalability.

TABLE 3. Probabilities Worn for Performance Sensitivity

S.No.	Action	Probability
1	Malicious nodes involvement	10%
2	Authenticating nodes	50%
3	Conversion from genuine to malicious	5%

V. SIMULATION RESULTS

In this section, the proposed framework is evaluated against existing baseline model depends on several performance criteria and metrics.

A. PERFORMANCE METRICS

In order to measure the proposed mechanism performance, we have considered several evaluation criteria including various metrics.

1) *Trust:* This metric is related to the trust indicating highly trusted parameter to ensure node's legitimacy. It is calculated via equation 7:

$$RT = \sum_{i=1}^{N}(MT + RE + AN + PL) \tag{7}$$

where, MT is message transmission, RE is residual energy, AN is authenticating nodes and PL is packet loss.

2) *Authentication Delay (Average/Maximum)*: it is defined as the maximum and average amount of time required to validate the participating and communicating number of nodes. It is a request delay which indicates the difference between time to authenticate and time made by requesting node.

$$AAD = \sum_{i=1}^{N} \frac{Time_{Rqst} - Time_{auth}}{Total\ number\ of\ requesting\ nodes} \tag{8}$$

3) *Message Alteration*: It is defined as a change in small or large information of data to perform malicious activities in the network.
4) *Brute force and Crypt analysis Attack*: It is defined as where attacker tries every possible way to obtain the information or message communication among the nodes without any knowledge of cryptographic key or hash.
5) *Throughput*: It is defined as at a given interval of time, the total number of information received by the

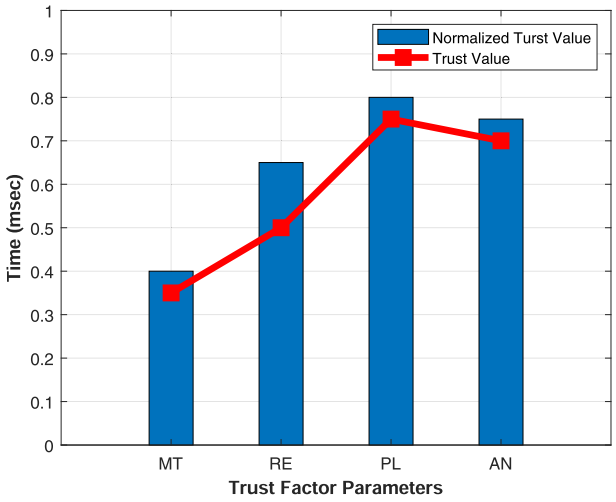

FIGURE 7. Relative weights of security parameter.

destination node. If T_{tp} are the information transmitted and T_{rp} are total number of information received, then throughput can be given as:

$$Network\ Throughput = \sum_{i=1}^{N} \frac{Total\ number\ of\ packets}{T_{tp} - T_{rp}} \tag{9}$$

B. EXISTING (Baseline) METHOD

We have compared the efficiency of our proposed framework against [28]. In this article in order to solve the risks related to voting fairness where individuals may cast their single vote twice, voting of non-candidates, tampered data and excessive authorities, it is necessary to further look over the security concerns of voting systems. The integration of Blockchain mechanism and voting system may reduces the mentioned risks with transparent and decentralized feature of Blockchain technology. [28] have proposed e-voting Blockchain system to maintain the transparency, limit the voting threats and audit the incorrect voter's operations using hash-based and certificates cryptographic mechanism. The proposed mechanism of the authors is suitable in the case where number of voters is less and voting is done at small scale.

C. RESULTS AND DISCUSSION

We have considered several parameters to compare our proposed phenomenon against existing (baseline) method. In traditional mechanism, malevolent nodes are measured using some cryptographic mechanisms that include the overall complexities and computational overhead of managing, storing of cryptographic keys.

However, in our proposed phenomenon, trust, message alteration, DoS attack and authentication process performs better as upon identification malicious nodes are immediately removed from the network. In order to measure legitimacy or misbehavior of nodes, the authors have analyzed a trust parameter. The trust value of nodes is dependent upon several metrics such as message transmission, residual energy, authenticating nodes and packet loss. The trust metric is related to the trust indicating highly trusted metric to ensure node's legitimacy. Figure 7 illustrates the relative normalized weights of several parameters. Message transmission and authenticating nodes have maximum relative weight in comparison of other metrics that indicates that these are the most significant parameter to identify the node's legitimacy.

Further, Figure 8 and 9 illustrate DoS and DDoS threats that are specific to e-voting and Blockchain framework. In depicted Figure 8, the proposed mechanism outperforms better because of Blockchain mechanism where nodes performing any malicious behavior or activity can be identi-

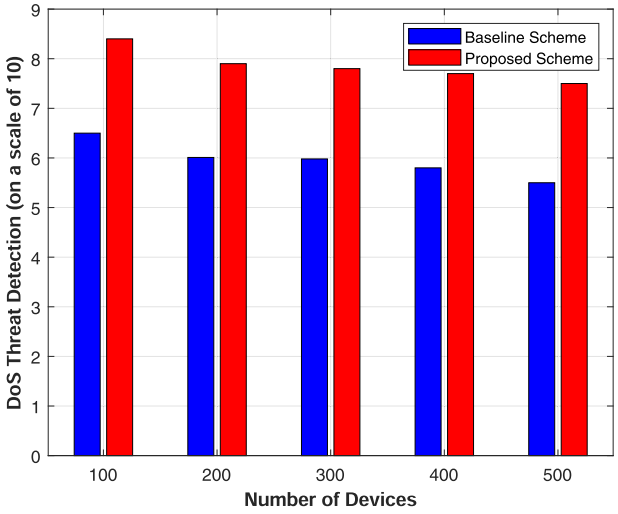

FIGURE 8. DoS threat detection over number of devices.

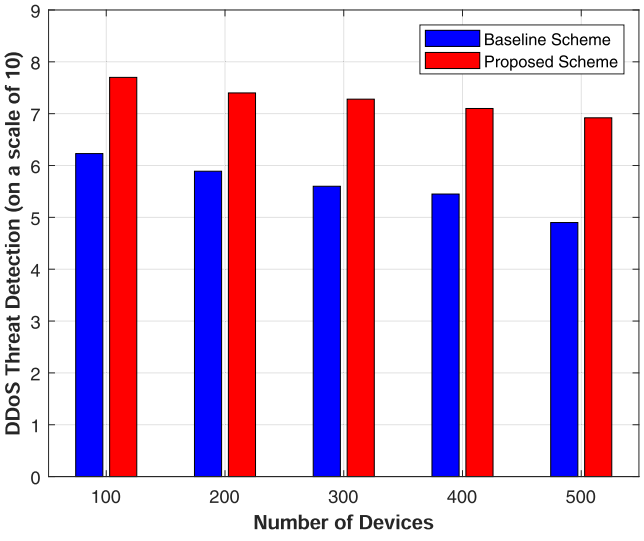

FIGURE 9. DDoS threat detection over number of devices.

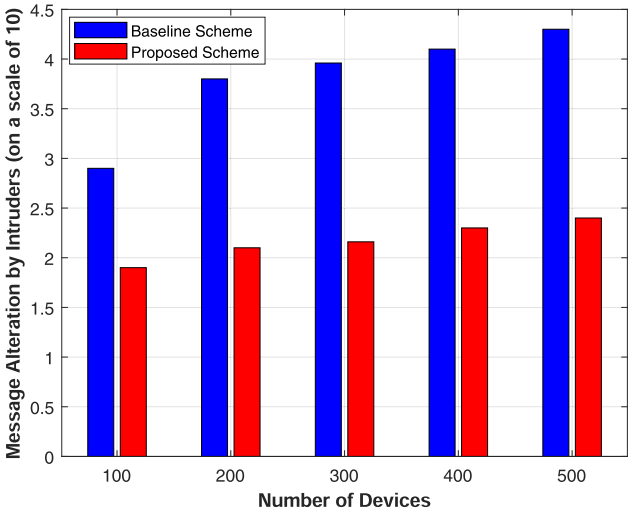

FIGURE 10. Message alteration over number of IoT devices.

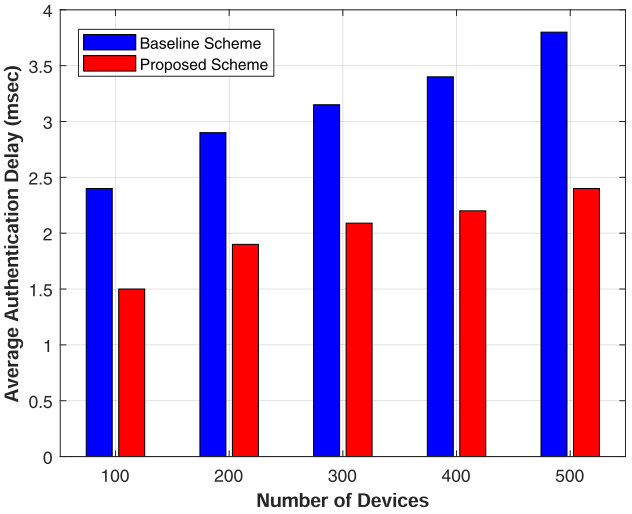

FIGURE 11. Average authentication delay.

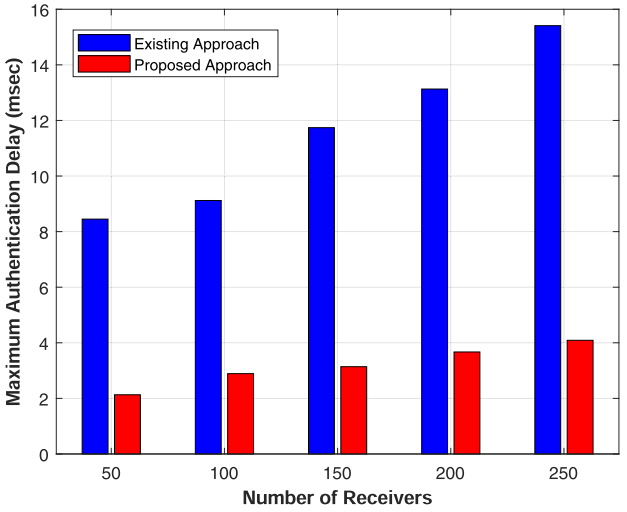

FIGURE 12. Maximum authentication delay.

fied and eliminated immediately from the communicating environment.

Similarly, Figure 9 represents DDoS attack where the permission and distributed nature of Blockchain mechanism such as election administrator responsible to allow the accessing permission to remaining levels and able to trace and look over every individuals genuine and malicious activity done by any entity. Further, as clearly seen in Figure 8 and 9, the x-axis values are decreasing in both proposed mechanism and baseline approaches. The reason is that during the initial establishment of network, malicious nodes may get involved in the communication process. However, once the network is established, the nodes are allowed in transmission process depending upon their trust values.

However, in comparison of baseline method, it becomes very difficult to detect, trace and prevent any malicious activity at an earliest stage. Further, distributed and permission environment reduces the overload on remaining number of level to store and manage huge database of information. Figure 10 represents message alteration attack where attackers try to alter or access the information communicating in the network.

Now, in this case, proposed mechanism performs better because election administrator has the permission to look over the entire environment and allows the remaining levels to access the information. The distributed and permission characteristics permits number of nodes have limited permission to trace and access the information among each other.

Finally, Figure 11 and 12 present average and maximum authentication delay of baseline and proposed e-voting mechanism over several numbers of devices. The authentication of malicious and legitimate devices through trust computation ensures fast and efficient detection process as compared to other baseline mechanism. The maximum and average authentication delay of both baseline and proposed approaches increase with the number of nodes. The reason is that as number of nodes increases, the time to authenticate the present nodes and newly joined nodes takes time to authenticate themselves because it is needed to check every node database before permitting them for communication.

VI. CONCLUSION

This article has initiated the concept of E-voting attacks that occur during polling mechanism in the smart cities. The privacy and security flaws are successfully resolved by computing the trust of each entity and further store them in a Blockchain to analyze their continuous behaviour when compared. Further, the proposed phenomenon shows significant improvement as compare to baseline scheme because proposed approach ensured security using blockchain and trust computation instead of verifying the certificates and applying cryptographic schemes. The proposed mechanism

is validated extensively against baseline mechanism by comparing various security parameters. Furthermore, the proposed mechanism has significantly outperformed the baseline mechanism by tracing the activity of every election process level. Further, the proposed framework shows better success rate in all simulation results against baseline mechanism over message alteration, DoS, DDoS threats and authentication mechanisms. The accuracy of proposed mechanism will be further validated and confirmed over real-time data set in future communication.

REFERENCES

[1] P. Lombardi, S. Giordano, H. Farouh, and W. Yousef, "Modelling the smart city performance," *Innov., Eur. J. Social Sci. Res.*, vol. 25, no. 2, pp. 137–149, Jun. 2012.

[2] P. Neirotti, A. De Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, "Current trends in smart city initiatives: Some stylised facts," *Cities*, vol. 38, pp. 25–36, Jun. 2014.

[3] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-based smart cities: Recent advances and challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16–24, Sep. 2017.

[4] M. E. M. Cayamcela and W. Lim, "Artificial intelligence in 5G technology: A survey," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2018, pp. 860–865.

[5] F. Al-Turjman, "5G-enabled devices and smart-spaces in social-IoT: An overview," *Future Gener. Comput. Syst.*, vol. 92, pp. 732–744, Mar. 2019.

[6] R. Molina-Masegosa and J. Gozalvez, "LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 30–39, Dec. 2017.

[7] P. Tarasov and H. Tewari, "The future of E-voting," *IADIS Int. J. Comput. Sci. Inf. Syst.*, vol. 12, no. 2, pp. 1–19, 2017.

[8] N. Kshetri and J. Voas, "Blockchain-enabled E-voting," *IEEE Softw.*, vol. 35, no. 4, pp. 95–99, Jul. 2018.

[9] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[10] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[11] K. Curran, "E-voting on the blockchain," *J. Brit. Blockchain Assoc.*, vol. 1, no. 2, pp. 1–6, Dec. 2018.

[12] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Comput. Secur.*, vol. 94, Jul. 2020, Art. no. 101863.

[13] M. Shafiq, X. Yu, A. K. Bashir, H. N. Chaudhry, and D. Wang, "A machine learning approach for feature selection traffic classification using security analysis," *J. Supercomput.*, vol. 74, no. 10, pp. 4867–4892, Oct. 2018.

[14] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[15] U. D. Gandhi, P. M. Kumar, R. Varatharajan, G. Manogaran, R. Sundarasekar, and S. Kadu, "HIoTPOT: Surveillance on IoT devices against recent threats," *Wireless Pers. Commun.*, vol. 103, no. 2, pp. 1179–1194, Nov. 2018.

[16] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, pp. 1–15, 2019.

[17] M. Abdur, S. Habib, M. Ali, and S. Ullah, "Security issues in the Internet of Things (IoT): A comprehensive study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, p. 383, 2017.

[18] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based E-voting system," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 983–986.

[19] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, pp. 1–22, 2019.

[20] X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang, and J. Piran, "Blockchain-based incentive energy-knowledge trading in IoT: Joint power transfer and AI design," *IEEE Internet Things J.*, early access, Sep. 15, 2020, doi: 10.1109/JIOT.2020.3024246.

[21] J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A. K. Bashir, and R. Nawaz, "Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4478–4488, Aug. 2020.

[22] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "A secure verifiable ranked choice online voting system based on homomorphic encryption," *IEEE Access*, vol. 6, pp. 20506–20519, 2018.

[23] A. Meraoumia, H. Bendjenna, M. Amroune, and Y. Dris, "Towards a secure online E-voting protocol based on palmprint features," in *Proc. 3rd Int. Conf. Pattern Anal. Intell. Syst. (PAIS)*, Oct. 2018, pp. 1–6.

[24] D. F. Aranha and J. van de Graaf, "The good, the bad, and the ugly: Two decades of E-voting in Brazil," *IEEE Secur. Privacy*, vol. 16, no. 6, pp. 22–30, Nov. 2018.

[25] A. Qureshi, D. Megías, and H. Rifà-Pous, "SeVEP: Secure and verifiable electronic polling system," *IEEE Access*, vol. 7, pp. 19266–19290, 2019.

[26] A. O. Santin, R. G. Costa, and C. A. Maziero, "A three-ballot-based secure electronic voting system," *IEEE Secur. Privacy Mag.*, vol. 6, no. 3, pp. 14–21, May 2008.

[27] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkiliç, "Towards secure E-voting using Ethereum blockchain," in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–7.

[28] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum E-voting protocol in blockchain with audit function," *IEEE Access*, vol. 7, pp. 115304–115316, 2019.

[29] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019.

[30] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Gener. Comput. Syst.*, vol. 86, pp. 650–655, Sep. 2018.

GEETANJALI RATHEE received the Ph.D. degree in computer science engineering from the Jaypee University of Information Technology (JUIT), Waknaghat, India, in 2017. She is currently an Assistant Professor with the Department of Computer Science Engineering and Information Technology, JUIT. She has approximately 25 publications in peer-reviewed journals and more than 15 publications in international and national conferences. Her research interests include handoff security, cognitive networks, blockchain technology, resilience in wireless mesh networking, routing protocols, networking, and industry 4.0. She is also a reviewer for various journals such as the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, *Wireless Networks*, *Cluster Computing*, *Ambience Computing*, *Transactions on Emerging Telecommunications Engineering*, and the *International Journal of Communication Systems*.

RAZI IQBAL (Senior Member, IEEE) received the master's and Ph.D. degrees in computer science and engineering from Akita University, Akita, Japan. His prior work includes an Associate Professorship with the College of Computer Information Technology, American University in the Emirates, Dubai, United Arab Emirates. He has also served as the Chairman for the Department of Computer Science and IT and also the Director for the Office of Research, Innovation and Commercialization and Research Scientist at various academic institutes. He is currently a Faculty Member with the Department of Computer Information Systems, University of the Fraser Valley, Canada. His current research interests include short range wireless technologies in precision agriculture, transportation, and education.

Dr. Razi currently a member of the IEEE Computer and Computational Society. He serves as an editor and reviewer for several peer-reviewed journals.

OMER WAQAR (Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Engineering and Technology (UET), Lahore, Pakistan, in 2007, and the Ph.D. degree in electrical and electronic engineering from the University of Leeds, Leeds, U.K., in November 2011. From January 2012 to July 2013, he was a Research Fellow with the Center for Communications Systems Research and 5G Innovation Center (5GIC), University of Surrey, Guildford, U.K. From August 2013 to June 2018, he was also an Assistant Professor with UET. From July 2018 to June 2019, he was a Researcher with the Department of Electrical and Computer Engineering, University of Toronto, Canada. Since August 2019, he has been an Assistant Professor with the Department of Engineering, Thompson Rivers University (TRU), BC, Canada. He has published 17 peer-reviewed articles including top-tier journals such as the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and received more than 175 citations according to the Google scholar. His current research interests include energy-efficient design of future-generation wireless access networks, intelligent reflecting surface aided communication systems, deep-learning, and security for next generation communication systems.

ALI KASHIF BASHIR (Senior Member, IEEE) received the B.Sc. degree (Hons.) in computer forensics and security from the Department of Computing and Mathematics, Manchester Metropolitan University, U.K., and the Ph.D. degree in computer science and engineering from Korea University, South Korea. His past assignments include an Associate Professor of ICT, University of the Faroe Islands, Denmark; Osaka University, Japan; the Nara National College of Technology, Japan; the National Fusion Research Institute, South Korea; Southern Power Company Ltd., South Korea, and Seoul Metropolitan Government, South Korea. He has worked on several research and industrial projects of South Korean, Japanese, and European agencies and Government Ministries. He is currently a Senior Lecturer/Associate Professor and a Course Leader of the Department of Computing and Mathematics, Manchester Metropolitan University. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, National University of Science and Technology (NUST), Islamabad, and also as an Affiliated Professor with the School of Information and Communication Engineering, University of Electronics Science and Technology of China (UESTC), where he is also a Chief Advisor of the Visual Intelligence Research Center. He has authored more than 180 research articles; received funding as PI and Co-PI from research bodies of South Korea, Japan, EU, U.K., and Middle East; supervising/co-supervising several graduate (M.S. and Ph.D.) students. His research interests include the Internet of Things, wireless networks, distributed systems, network/cyber security, network function virtualization, and machine learning.

Dr. Bashir is a member of the IEEE Industrial Electronic Society and of ACM, and a Distinguished Speaker of ACM. He is also leading many conferences as a chair (program, publicity, and track) and had organized workshops in flagship conferences like IEEE INFOCOM, IEEE GLOBECOM, and IEEE MOBICOM. He is serving as the Editor-in-Chief for the *IEEE Future Directions Newsletter*. He is also serving as an Area Editor for *KSII Transactions on Internet and Information Systems* and also an Associate Editor for the *IEEE Internet of Things Magazine*, IEEE ACCESS, *IET Quantum Computing*, and the *Journal of Plant Disease and Protection*.